Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **NOV 2011**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE
Fault Tolerance for Fight-Through: A Basis for Strategic Survival

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory Cyber Science Branch Rome, NY 13441

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA553912. International Conference on Security of Information and Networks (4th) (SIN 2011) Held in Sydney, Australia on November 14-19, 2011. Approved for public release; U.S. Government or Federal Purpose Rights License.

14. ABSTRACT
Concepts from the domain of fault-tolerant computing cannot be merely adopted for cyber defense; instead they have to be adapted.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**2**	

Fault Tolerance for Fight-Through: A Basis for Strategic Survival

Kevin A. Kwiat
Air Force Research Laboratory
Cyber Science Branch
Rome, NY 13441
315-330-1692
kwiatk@rl.af.mil

ABSTRACT

Concepts from the domain of fault-tolerant computing cannot be merely adopted for cyber defense; instead they have to be *adapted*.

Categories and Subject Descriptors

C.2.3 [Network Operations]: Network management; D.4.6 [Security and Protection]: Access Controls; K.6.5 [Security and Protection]: Invasive software

General Terms

Reliability, Security

Keywords

Fault Tolerance, Survivability, Fight-Through

1. INTRODUCTION

The 1st Workshop on Survivability in Cyberspace [1] was sponsored by the Air Force Office of Scientific Research (AFOSR) and held as part of CPSWeek 2010. Cyber-physical systems (CPS) are engineered systems whose operations are monitored, coordinated, controlled, and integrated by a computing and communication core and embedded in all types of objects and structures in the physical environment. The workshop not only called attention to the need for such systems to operate safely, dependably, securely, efficiently, and in real-time, but also underscored the Air Force's mission that encompasses air, space and cyber. Among the triad of air-space-cyber, the settings of the latter differ primarily from the former two in a fundamental way: air and space are natural settings, but cyber is man-made. As a man-made entity, cyber is composed of networking and information resources – and is therefore subject to human control. Because of this distinction, the human ability to create and sustain cyber-level linkages can become a venue for malice.

2. CYBER DEFENSE

Defense of cyberspace is challenging. The seemingly endless breadth of cyberspace coupled with the technological depth of its composition can divide defensive approaches to be either overarching or highly specific. In order to abstract away details for the purpose of tractability, overarching approaches can suffer because simplistic models for threats, vulnerabilities, and exploits tend to yield defenses that are too optimistic. Approaches that deal with specific threats, vulnerabilities and exploits may be more credible but can quickly lose their meaningfulness as technology changes. Whether approaches are near-or-far term, we see that two underlying attributes remain essential: the ability to survive and the ability to fight-through.

When a cyber defense's ability to predict, prevent, avoid, and detect an attack are outmaneuvered and information systems face impending loss of critical services, a fight-through capability must remain; otherwise restoration of those services may come too late to emerge undefeated. The task of "protecting the protector" drives us to create a fight-through capability that is hardened and heavily defended in cyberspace; however, these attributes alone become an instantiation of a "Maginot Line". Such a strict bastion mentality should be replaced by one that advocates agility. Our goal then becomes more realistic: to design a fight-through capability that can absorb punishment and *reacts* by rebounding to serve as the basis for restoration of critical services.

We liken the fight-through problem to an Observe, Orient, Decide, and Act (OODA) loop. Redundancy, as the underpinning of fault tolerance, is strategically placed to counter an attacker's optimal strategies. The aim of a fight-through OODA loop is to outperform the adversary's OODA loop.

3. STRATEGIC SURVIVAL

We cast using fault tolerance for fight-through (FTFT) as seeking collective judgments among replicated tasks (hereby referred to as replicas) in a cloud computing environment. The goal is an optimum strategy for replicas to survive and fight through a strategically created attack. Operationally, replicas stay in synch through consensus, so it is important to realize that monitoring of the consensus protocol's message flow can, over time, reveal to the attackers their sought-after target. We envision the adversary's OODA loop to be this: *observe* the message flow; *orient* an attack to the target; *decide* when and how to attack; and then *act* by launching the attack. The fight-through OODA loop will counter our adversary by providing resources to: *observe* the attack on any of replicas; *orient* the replicas toward a new random configuration; *decide* on randomizing before the configuration is overwhelmed; and then to *act* by dispersing it in the cloud. Our use of redundant resources allows execution of the fight-through

SIN'11, November 14–19, 2011, Sydney, Australia.
ACM 978-1-4503-1020-8/11/11.

OODA loop prior to our adversaries completing their OODA loop on *all* of the replicas. To defeat the fight-through OODA loop, the attack must succeed against a majority of replicas simultaneously.

FTFT's uses redundancy primarily as a vehicle for tolerating attacker-induced faults. However, a journal article [4] shows that hiding a small fraction of the information about a network's nodes dramatically improves the overall survivability of the network when it is attacked. Adopting this approach, FTFT's underlying redundancy potentially offers hiding places for information about the network. By fulfilling this potential, FTFT can be the basis for additional defensive strategies..

4. CONCLUSION

Our interest in creating a fight-through capability involves a critical analysis of redundancy to establish a fight-through OODA loop that outperforms our attacker's OODA loop. By being able to *observe* an attacker's attempts to create faults, FTFT will *orient* the replicas and *decide* on their deployment in order to *act* against the attack – by fighting through it.

5. BIOGRAPHY

Kevin A. Kwiat is a Principal Computer Engineer in the Cyber Science Branch of the U.S. Air Force Research Laboratory (AFRL) in Rome, New York where he has worked for over 28 years. He received the Ph.D. in Computer Engineering from Syracuse University. He holds 4 patents. In addition to his duties with the Air Force, he is an adjunct professor of Computer Science at the State University of New York at Utica/Rome, an adjunct instructor of Computer Engineering at Syracuse University, and a Research Associate Professor with the University at Buffalo. He completed assignments as an adjunct professor at Utica College of Syracuse University, a lecturer at Hamilton College, a visiting scientist at Cornell University, and as a visiting researcher at the University of Edinburgh as part of the Air Force Office of Scientific Research "Window on Europe" program. He has been by recognized by the AFRL Information Directorate with awards for best paper, excellence in technology teaming, and for outstanding individual basic research.

6. ACKNOWLEDGMENTS

This research was supported by the Air Force Office of Scientific Research. Approved for Public Release; Distribution Unlimited: 88ABW-2011-4932.

7. REFERENCES

[1] Kwiat, K. and Hurley, P. 2011. Survivability in Cyberspace Workshop: Learning How to Fight Through. *IAnewsletter*, Vol. 14, No. 1, Information Assurance Technology Analysis Center, Winter 2011.

[2] Leversage, D. and Byres, E. 2008. Estimating a System's Mean Time-to-Compromise. *Journal of Security and Privacy*, Vol. 6, Issue1, IEEE, 2008.

[3] Jonsson, E. and Olovsson. T. 1997. A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior. *IEEE Transactions of Software Engineering*, Vol. 23, No. 4, 1997.

[4] Wu J., Deng, H., Tan Y., and Zhu, D. 2007. Vulnerability of Complex Networks Under Intentional Attack with Incomplete Information. *Journal of Physics A: Mathematical and Theoretical*, Vol. 40, IOP Publishing, 2007.